UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

27871 7590 03/20/2007

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/025,924	VANSTONE ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 are pending.

2. Response filed 03/05/2007 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (US 6195433) (hereinafter Vanstone) in view of Schneier (Applied Cryptography) and further in view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas).

As per claim 1, Vanstone discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see column 3 lines 37-39); performing a hash function on said seed value to provide an output (see column 3 lines 41-45); determining if the outputted value is accepted or rejected (see

column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see column 3 line 51 through column 4 line 44); and if the output is accepted, providing the key for use in performing said cryptographic function wherein said key is equal to said output (see column 3 lines 37-45).

Vanstone fails to disclose the steps of determining and accepting/rejecting based on an order q.

However, Schneier teaches the steps of accepting/rejecting based on an order q (see page 487 lines 12-15 and line 11) and Matyas teaches determining whether an output is less than a prime number q (see column 6 line 65 through column 8 line 35).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Schneier and Matyas in the key generation system of Vanstone.

Motivation to do so would have been to use the well-known DSA (see Schneier pages 486-487) and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6).

As per claim 2, the modified Vanstone, Schneier, and Matyas system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page

487 line 11; Page 489, line 22 and Vanstone column 3 line 51 through column 4 line 44).

As per claim 4, the modified Vanstone, Schneier, and Matyas system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8 and Vanstone column 4 lines 45-48).

As per claim 5, the modified Vanstone, Schneier, and Matyas system discloses a method wherein said order q is prime number represented by a bit string of predetermined length L (see Schneier age 487, line 1 and Page 488, line 5).

5. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Vanstone, Schneier, and Matyas system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Vanstone, Schneier, Matyas, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Vanstone, Schneier, and Matyas system discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see Vanstone column 3 lines 37-39); performing a hash function on said seed value to provide an output (see Vanstone column 3 lines 41-45); determining if the outputted value is accepted or rejected (see Vanstone column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see Vanstone column 3 line 51 through column 4 line 44); and if the output is accepted,

providing the key for use in performing said cryptographic function wherein said key is equal to said output (see Vanstone column 3 lines 37-45). The determination and accepting/rejection based on the order q being taught by Schneier and Matyas as applied to claim 1.

The modified Vanstone, Schneier, and Matyas system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q.

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using

the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Vanstone, Schneier, Matyas, and Backal system wherein a bit string greater than a predetermined length L is obtained and an L bit string selected therefrom for comparison with said order q (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Vanstone, Schneier, Matyas, and Backal system wherein upon rejection of said bit string of predetermined length L, a further L bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

6. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Vanstone, Schneier, and Matyas system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.

As per claim 6, the modified Vanstone, Schneier, and Matyas system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the

predetermined output length in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Vanstone, Schneier, Matyas, and Backal system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to form a predetermined length in the modified Vanstone, Schneier, Matyas, and Backal system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

7. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (Applied Cryptography) in

view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas) and further in view of Patel (US 6327660).

As per claim 1, Schneier discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is accepted or rejected based on an order q (see page 487 lines 12-15).

Schneier fails to disclose performing a hash function on seed number to provide an output, determining whether said output is less than said prime number q and repeating the method if the key is rejected and using the accepted key to perform a cryptographic function.

However, Matyas teaches performing a hash of each of seed values with SHA-I to produce hash values (see column 6, lines 7-9) and determining whether an output is less than a prime number q (see column 6 line 65 through column 8 line 35) and Patel teaches repeating the method if the key is rejected and using the accepted key to perform a cryptographic function (see column 6 lines 26-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Matyas and the repeating of Patel in the system of Schneier.

Motivation to do so would have been to and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6) and to produce keys which are not weak (see Patel column 6 lines 26-47).

As per claim 2, the modified Schneier, Matyas, and Patel system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page 487 line 11; Page 489, line 22).

As per claim 4, the modified Schneier, Matyas, and Patel system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8).

As per claim 5, the modified Schneier, Matyas, and Patel system discloses a method wherein said order q is prime number represented by a bit string of predetermined length L (see Schneier age 487, line 1 and Page 488, line 5).

8. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Schneier, Matyas, and Patel system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function

is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Schneier, Matyas, Patel, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Schneier, Matyas, and Patel system discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is

accepted or rejected based on an order q (see page 487 lines 12-15). The hashing, determining and repeating are as taught in claim 1 by Matyas and Patel.

The modified Schneier, Matyas, and Patel system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q.

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any

unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Schneier, Matyas, Patel, and Backal system wherein a bit string greater than a predetermined length L is obtained and an L bit string selected therefrom for comparison with said order q (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Schneier, Matyas, Patel, and Backal system wherein upon rejection of said bit string of predetermined length L, a further L bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

9. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel

system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Schneier, Matyas, and Patel system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.

As per claim 6, the modified Schneier, Matyas, and Patel system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the predetermined output length in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Schneier, Matyas, and Patel system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to form a predetermined length in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

Response to Arguments

10. Applicant's arguments filed 03/05/2007 have been fully considered but they are not persuasive. Applicant argues Schneier fails to teach using the output value as a key;

Vanstone teaches checking that the order is greater than a value, not lower; and the remaining references fail to make up for these deficiencies.

With respect to Applicant's argument that Schneier (when combine with Vanstone and Matyas or Matyas and Patel) fails to use the random value k as a key, this section of Schneier is describing the DSA algorithm and the value k is an ephemeral key. Applicant's specification also describes the DSA algorithm in a similar manner as Schneier and in line 16 specifically discloses that the value k is an ephemeral key. Therefore, the value k in Schneier is used as a key for use in a cryptographic function.

With respect to Applicant's argument that Vanstone teaches checking that the order is greater than a value, not lower, Examiner agrees, but when combined with Schneier (and Matyas) the system teaches choosing a value to be a key when it is greater than a value and less than a value. Therefore, the combination of Vanstone, Schneier and Matyas teach all of the limitations of claims 1, 2, 4, and 5.

Applicant's arguments that the remaining references fail to make up for the described deficiencies are moot in view of the above response.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shimbo and Pastor disclose methods of checking the order of a value before using it in a cryptographic system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner

can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER